

---

## *S3(Simple Storage Service)*

---

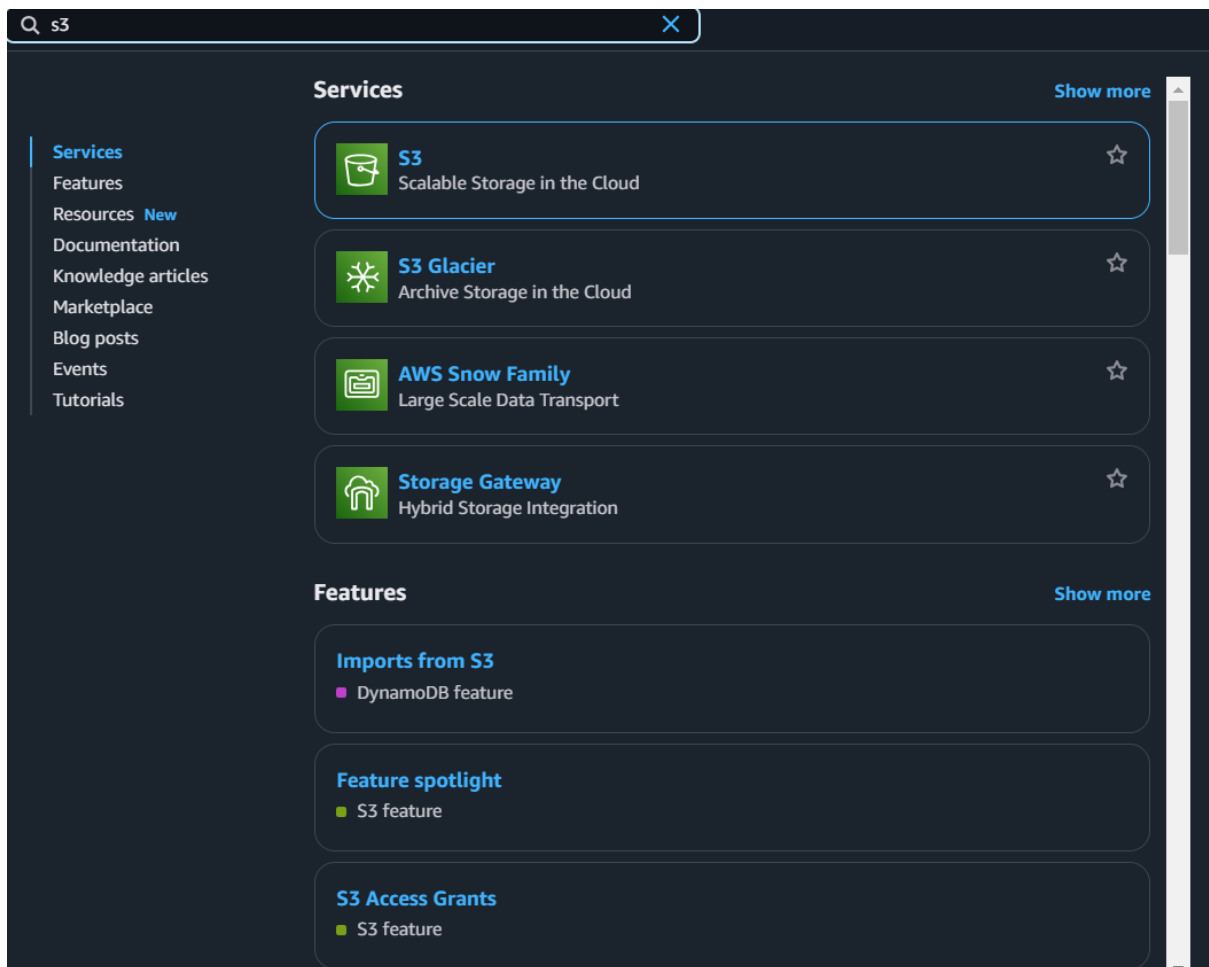
**Amazon S3 (Simple Storage Service)** is a scalable object storage service offered by AWS (Amazon Web Services). It is designed to store and retrieve large amounts of data, ranging from a few kilobytes to petabytes. S3 is commonly used for backup, data archiving, content distribution, and hosting static websites.

### **Key Features of Amazon S3:**

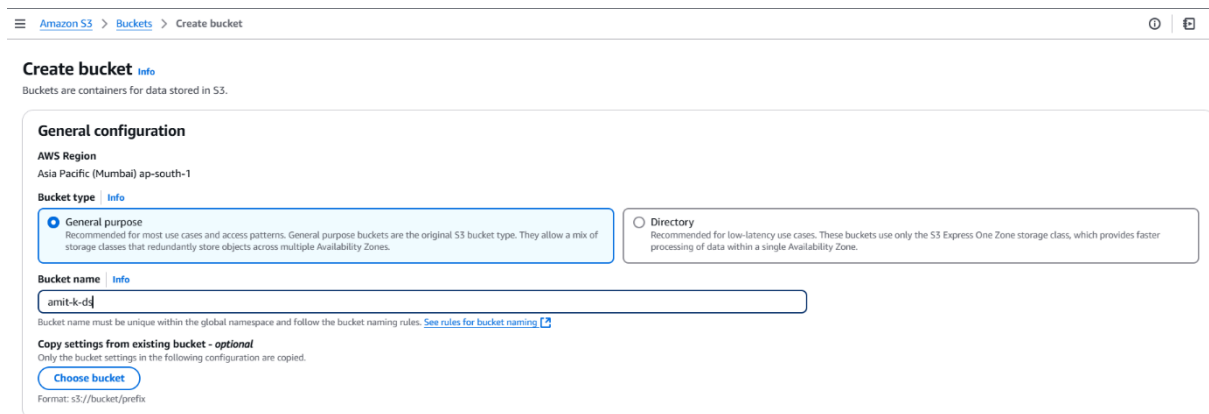
1. **Durability and Availability:** Provides high durability (99.999999999% or 11 9's) and availability for stored objects.
2. **Scalability:** Automatically scales to handle growing data and requests.
3. **Cost-Effectiveness:** Pay-as-you-go pricing model, with tiered storage options.
4. **Data Security:** Supports encryption (server-side and client-side) and fine-grained access control via IAM policies and bucket policies.
5. **Integration:** Easily integrates with other AWS services like EC2, Lambda, Athena, and Redshift.

➤ **Here, are visual steps :**

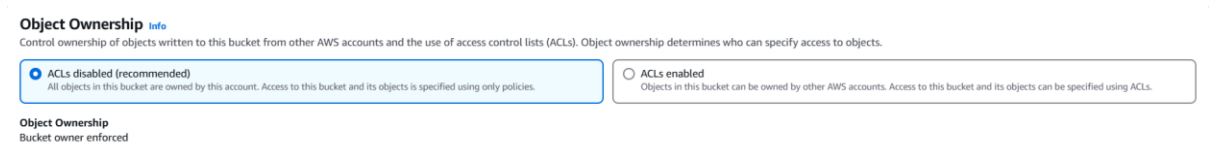
### **# Steps 1:**



## # Step 2:



## # Step 3:



## # step 4:

#### Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

##### ☒ Block all public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

##### ☒ Block public access to buckets and objects granted through new access control lists (ACLs)

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

##### ☒ Block public access to buckets and objects granted through any access control lists (ACLs)

S3 will ignore all ACLs that grant public access to buckets and objects.

##### ☒ Block public access to buckets and objects granted through new public bucket or access point policies

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

##### ☒ Block public and cross-account access to buckets and objects through any public bucket or access point policies

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

## # Step 5:

#### Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

##### Bucket Versioning

☒ Disable

☐ Enable

## # step 6:

### Tags - optional (0)

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.

Add tag

## # Step 7:

#### Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

##### Encryption type [Info](#)

☒ Server-side encryption with Amazon S3 managed keys (SSE-S3)

☐ Server-side encryption with AWS Key Management Service keys (SSE-KMS)

☐ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the [Storage](#) tab of the [Amazon S3 pricing page](#).

##### Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

☐ Disable

☒ Enable

## # Step 8:

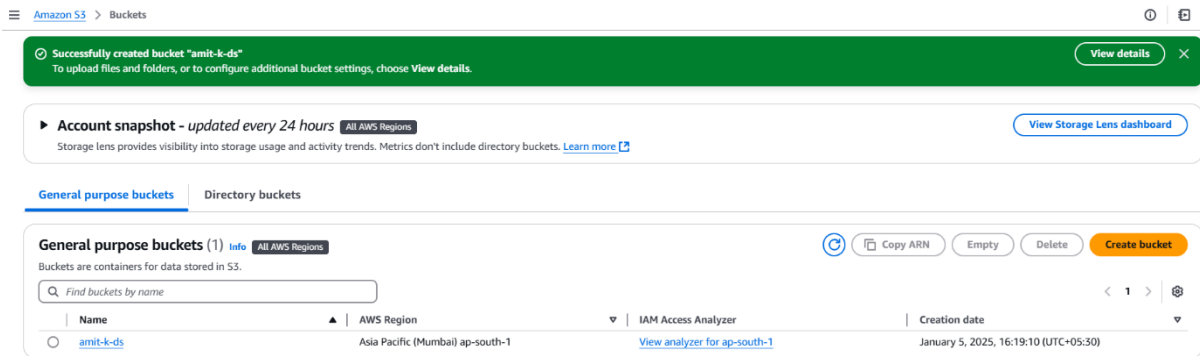
##### ► Advanced settings

① After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

[Cancel](#)

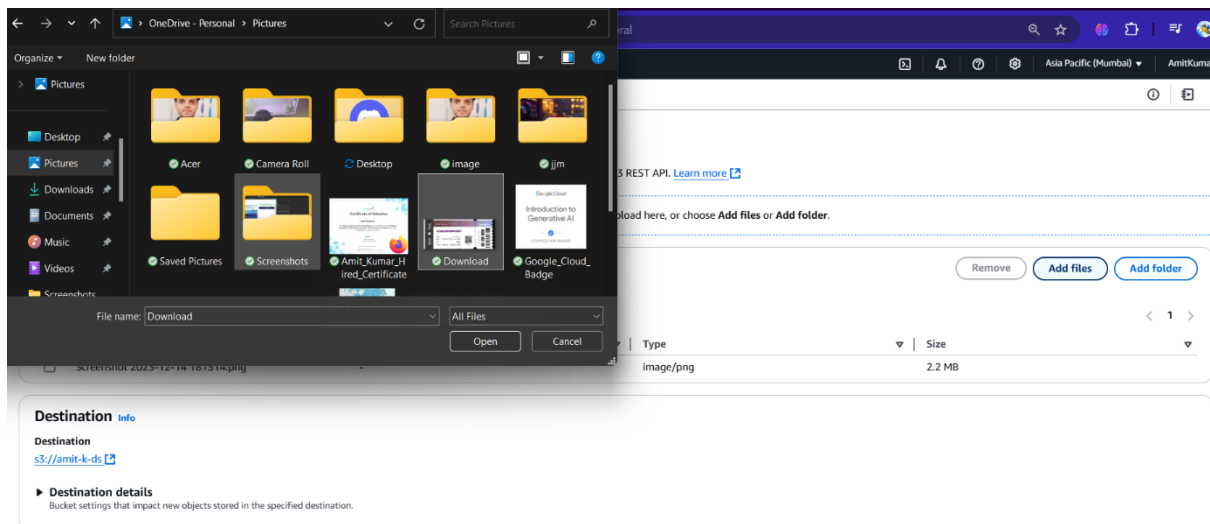
Create bucket

## # Step 9:



# now I'm storing data in the bucket.

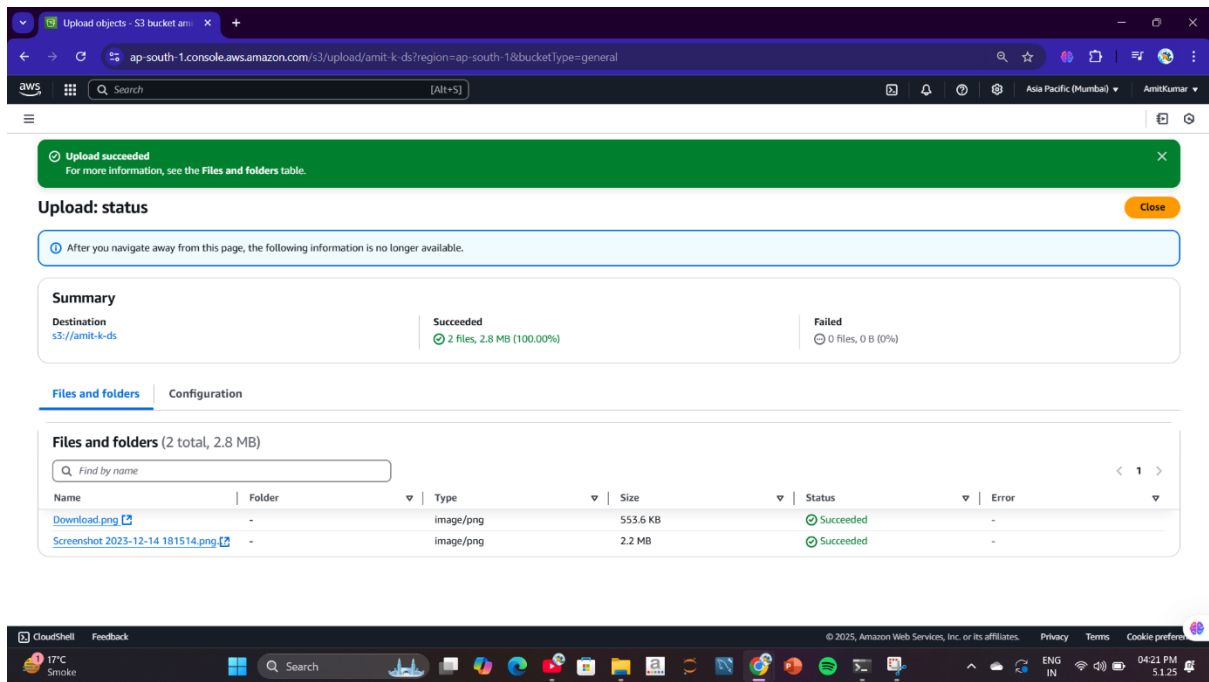
# Step 10:



# Step 11:

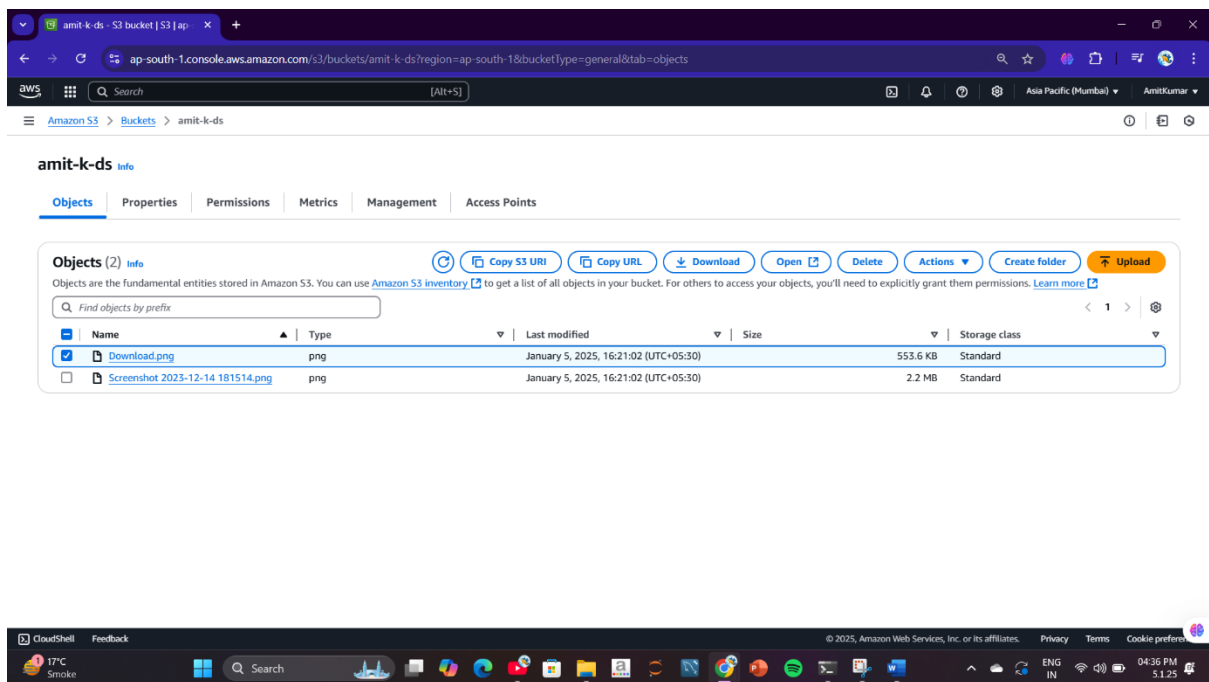


# Step 12:

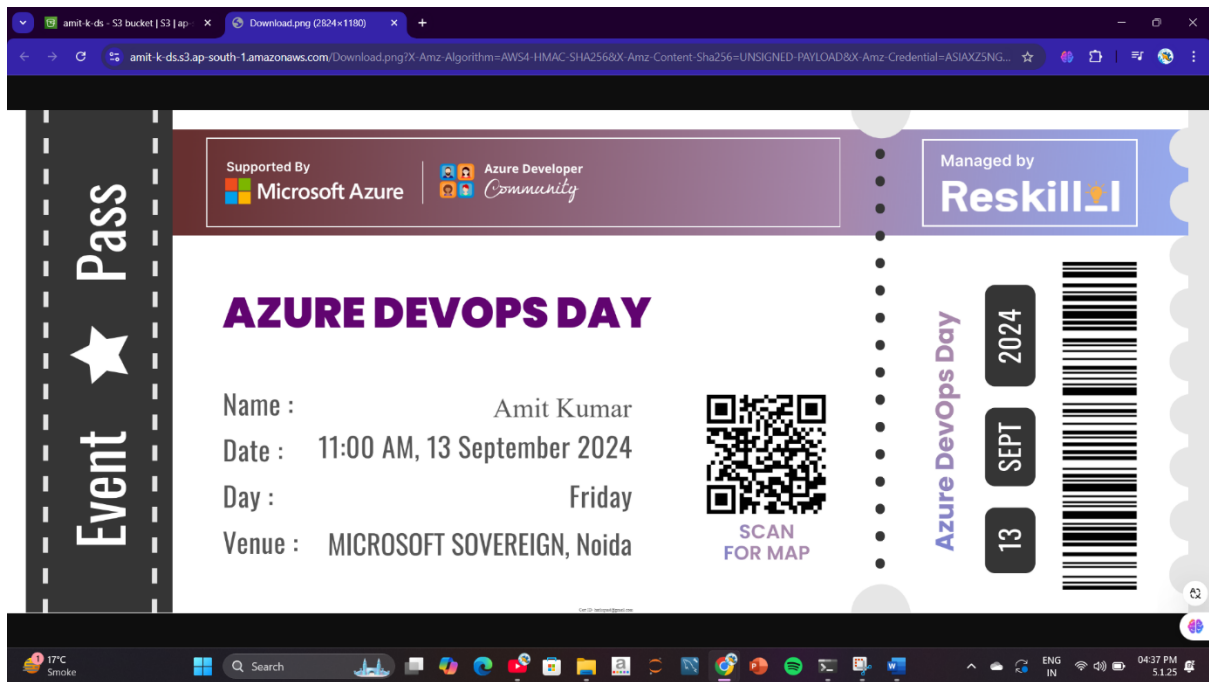


# So, I've uploaded the image. You can access the image firstly you will select the image and then click "Open" Button.

# Step 13:

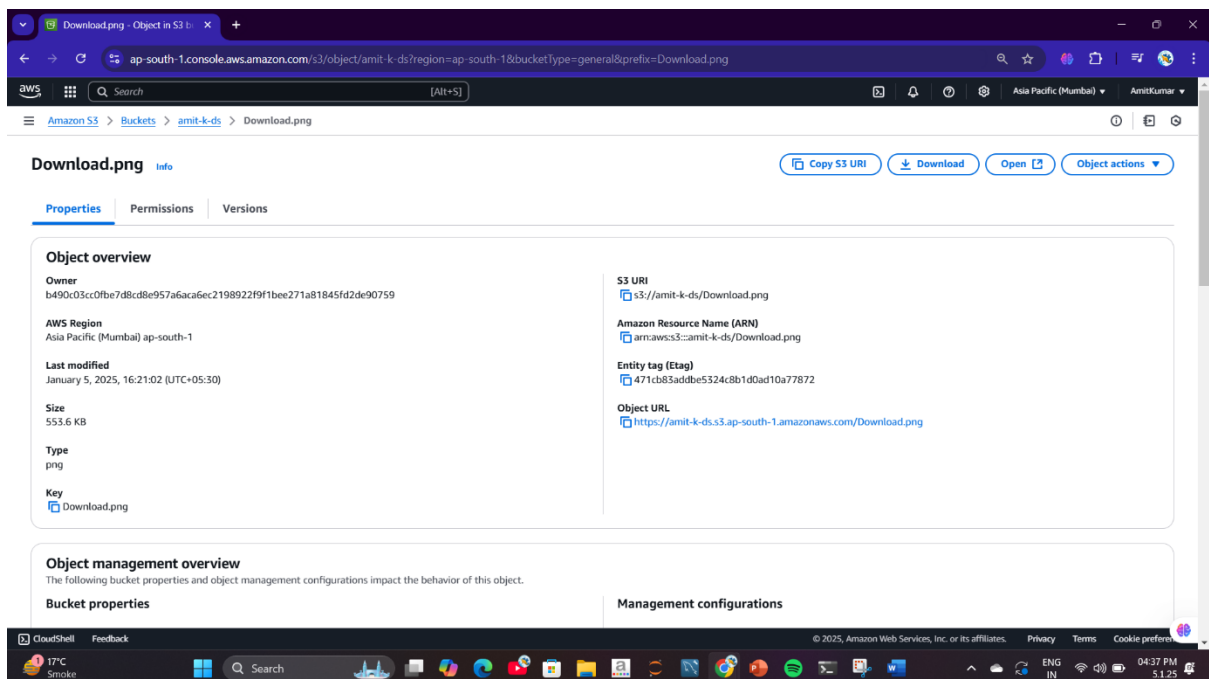


# Step 14:

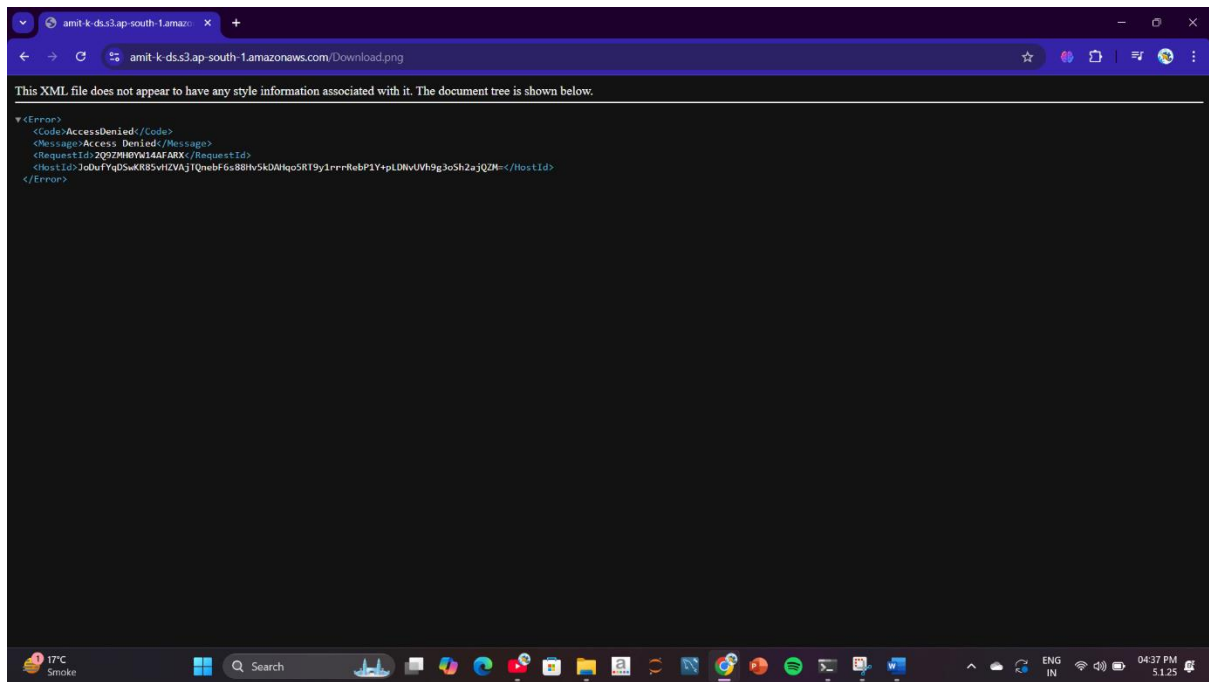


## # Step 15:

# if you click the object, So this page will open. Now I want to access the object by “Object URL” if you click Object URL It will give an error.

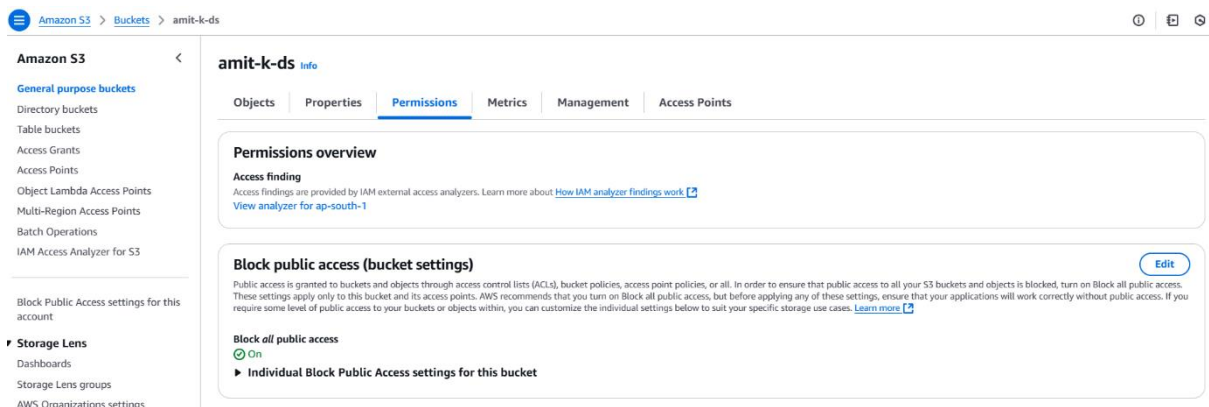


## # Step 16:



# here, are some steps you can handle it. this kind of problem.

# Step 17:



# Step 18:

Bucket policy

Edit
Delete

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

Public access is blocked because Block Public Access settings are turned on for this bucket

To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about [using Amazon S3 Block Public Access](#)

No policy to display.

Copy

# Step 19:

# I'll edit the bucket policy.

Edit bucket policy [info](#)

Bucket policy

Policy examples
Policy generator

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

Bucket ARN

arn:aws:s3:::amit-k-ds

Policy

1

Edit statement

Select a statement

Select an existing statement in the policy or

# Step 20:

# You have to create Bucket Policy.

### AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to [Amazon Web Services \(AWS\)](#) products and resources. For more information about creating policies, see [key concepts in Using AWS Identity and Access Management](#). Here are [sample policies](#).

#### Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an [IAM Policy](#), an [S3 Bucket Policy](#), an [SNS Topic Policy](#), a [VPC Endpoint Policy](#), and an [SQS Queue Policy](#).

Select Type of Policy S3 Bucket Policy

# Step 21:



## Step 2: Add Statement(s)

A statement is the formal description of a single permission. See [a description of elements](#) that you can use in statements.

**Effect** ☒ Allow ☐ Deny

**Principal**   
Use a comma to separate multiple values.

**AWS Service**  ☐ All Services ('\*')

Use multiple statements to add permissions for more than one service.

**Actions**  ☐ All Actions ('\*')

**Amazon Resource Name (ARN)**   
ARN should follow the following format: arn:aws:s3:::\${BucketName}/\${KeyName}.  
Use a comma to separate multiple values.

## # Step 21:

Principal(s)	Effect	Action	Resource	Conditions
• *	Allow	• s3:GetObject	arn:aws:s3:::amit-k-ds	None

## Step 3: Generate Policy

A *policy* is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

[Generate Policy](#) [Start Over](#)

## # Step 22:

### Policy JSON Document

Click below to edit. To save the policy, copy the text below to a text editor.  
Changes made below will **not be reflected in the policy generator tool**.

```
{
  "Id": "Policy1736075509029",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1736075440621",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amit-k-ds",
      "Principal": "*"
    }
  ]
}
```

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether

[Close](#)

## # Step 23:

### Block public access (bucket settings)

[Edit](#)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

#### Block all public access

On

► Individual Block Public Access settings for this bucket

## # Step 24:

## # I have to untick “Block Public Access”

### Edit Block public access (bucket settings) [Info](#)

#### Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

##### ☐ Block all public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

##### ☐ Block public access to buckets and objects granted through new access control lists (ACLs)

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

##### ☐ Block public access to buckets and objects granted through any access control lists (ACLs)

S3 will ignore all ACLs that grant public access to buckets and objects.

##### ☐ Block public access to buckets and objects granted through new public bucket or access point policies

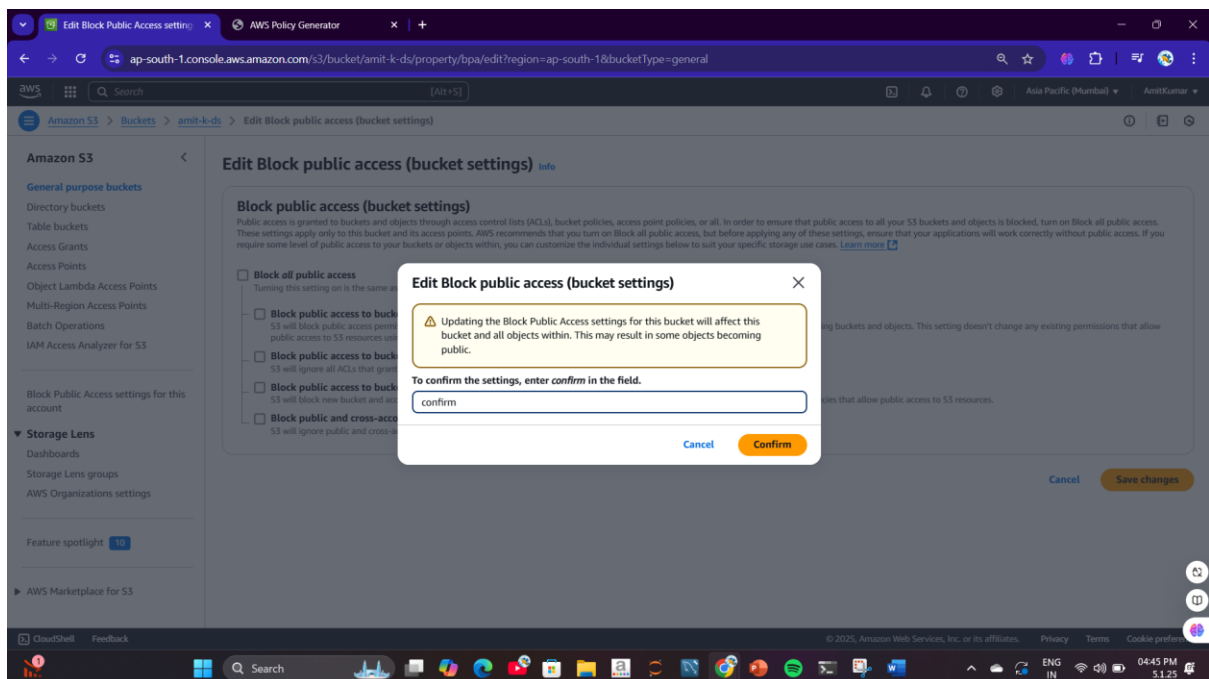
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

##### ☐ Block public and cross-account access to buckets and objects through any public bucket or access point policies

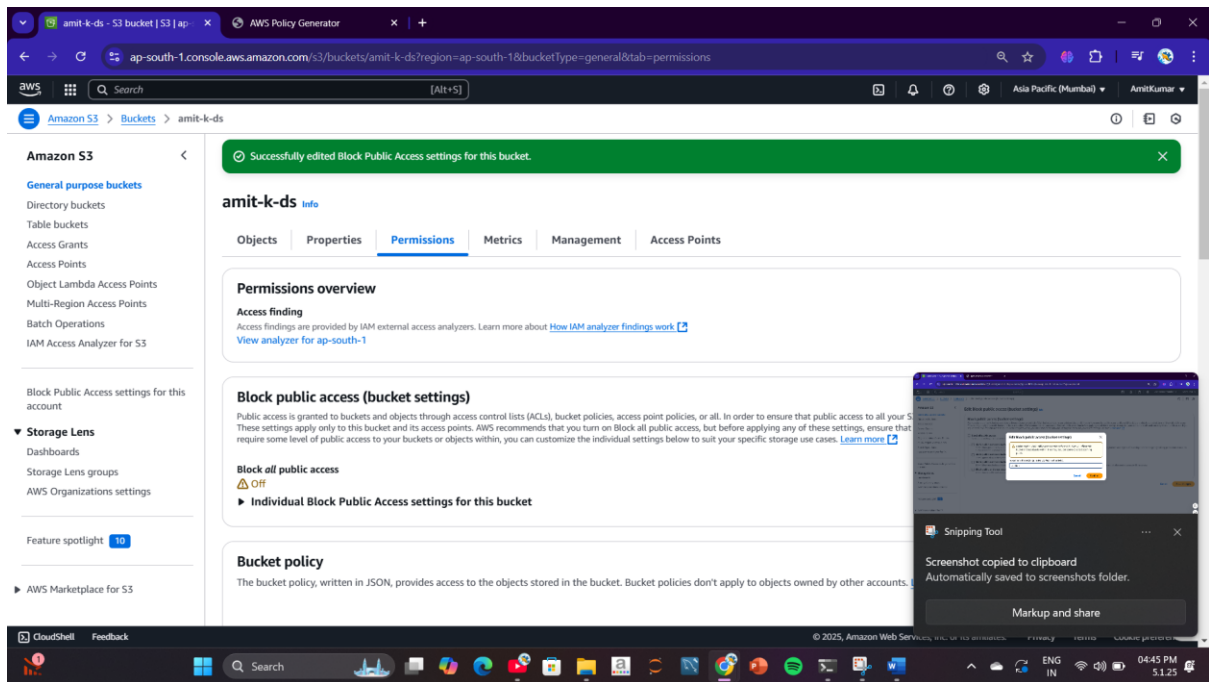
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

[Cancel](#)[Save changes](#)

## # Step 25:



## # Step 26:



# Step 27:

# This is the object.

